Improved Anonymous Broadcast Encryptions

Jiangtao Li, Junqing Gong

Improved Anonymous Broadcast Encryptions
Tight Security and Shorter Ciphertext

Jiangtao Li[1,⋆] and Junqing Gong[2,⋆⋆]

[1] East China Normal University, Shanghai, China
lijiangtao@stu.ecnu.edu.cn
[2] ENS de Lyon, Laboratoire LIP (U. Lyon, CNRS, ENSL, INRIA, UCBL), Lyon, France
junqing.gong@ens-lyon.fr

Abstract. We investigate anonymous broadcast encryptions (ANOBE) in which a ciphertext hides not only the message but also the target recipients associated with it. Following Libert *et al.*'s generic construction [PKC, 2012], we propose two concrete ANOBE schemes with tight reduction and better space efficiency.

- The IND-CCA security and anonymity of our two ANOBE schemes can be tightly reduced to standard k-Linear assumption (and the existence of other primitives). For a broadcast system with n users, Libert *et al.*'s security analysis suffers from $O(n^3)$ loss while our security loss is constant.
- Our first ANOBE supports fast decryption and has a shorter ciphertext than the fast-decryption version of Libert *et al.*'s concrete ANOBE. Our second ANOBE is adapted from the first one. We sacrifice the fast decryption feature and achieve shorter ciphertexts than Libert *et al.*'s concrete ANOBE with the help of bilinear groups.

Technically, we start from an instantiation of Libert *et al.*'s generic ANOBE [PKC, 2012], but we work out all our proofs from scratch instead of relying on their generic security result. This intuitively allows our optimizations in the concrete setting.

Keywords: broadcast encryption, full anonymity, chosen-ciphertext security, tight reduction, short ciphertext

⋆ Shanghai Key Laboratory of Trustworthy Computing, School of Computer Science and Software Engineering. Supported by the National Key R&D program of China (No. 2017YFB0802000) and NSF of China (Nos. 61572198, 61632012, 61672239). Part of this work was done while the author was visiting ENS de Lyon.

⋆⋆ Supported by the French ANR ALAMBIC project (ANR-16-CE39-0006).

Table of Contents

1 Introduction

Broadcast Encryption. *Broadcast encryption* [Ber91,FN94] (BE) is a public-key cryptosystem designed for securely sending information to multiple users via a public channel. In a BE system, we may index each user by integers $1, \ldots, n$ and name set $\mathcal{U} := \{1, \ldots, n\}$ the *universe*. It would be convenient to describe BE in the framework of *Functional Encryption* [BSW11]. An authority publishes a set of public parameters generated by the Setup algorithm. Each user's secret key is then created by the KeyGen algorithm from the master secret key which is the output of Setup. By invoking the encryption algorithm Enc, a sender can create a ciphertext for users specified by a target set $S \subseteq \mathcal{U}$. Any user with an index $i \in S$ is able to decrypt the ciphertext using the Dec algorithm.

The basic security requirement is *collusion-resistance* which ensures that a ciphertext leaks no information about the message even when multiple users outside the target set S decide to cooperate. More formally, it is required that

$$\{\mathsf{ct} \leftarrow_R \mathsf{Enc}(\mathsf{mpk}, S, m_0)\} \approx_c \{\mathsf{ct} \leftarrow_R \mathsf{Enc}(\mathsf{mpk}, S, m_1)\}$$

where mpk is the public parameters, $(S \subseteq \mathcal{U}, m_0, m_1)$ are chosen by the adversary; and we allow the adversary to adaptively learn secret keys for all $i \notin S$.

With more powerful functional encryptions such as attribute-based encryptions [SW05], [GPSW06,OT10,LOS+10,CGW15], we can securely broadcast information in a structural way which is more efficient and much easier to manage. However the classical BE still serves as the most general tool for broadcasting information in the systems where users are not well-organized, e.g., a country-wide pay-TV system.

Anonymity. Since been introduced, a series of BE schemes have been published [FN94], [NNL01,YFDL04,BGW05,DPP07,GW09,Wee16], but they only ensure the confidentiality of the message while the target set S is entirely exposed to the public. In fact, the description of S will be directly transmitted through the insecure channel for decryption. However in many applications, the confidentiality of the target set is also crucial. For instance, in the pay-TV setting, everyone has access to the full list of subscribers, which is not acceptable. Therefore, it is desirable and non-trivial to build a BE system taking both the message and the target set into account in terms of confidentiality. In this paper, we call the latter feature *anonymity* and name such a BE as *anonymous broadcast encryption* [LPQ12] (ANOBE). More formally, it is required that

$$\{\mathsf{ct} \leftarrow_R \mathsf{Enc}(\mathsf{mpk}, S_0, m_0)\} \approx_c \{\mathsf{ct} \leftarrow_R \mathsf{Enc}(\mathsf{mpk}, S_1, m_1)\}$$

where (m_0, m_1, S_0, S_1) are chosen by the adversary and secret keys for all $i \notin (S_0 \setminus S_1) \cup (S_1 \setminus S_0)$ can be revealed. The subtlety is that any secret key for $i \in S_0 \cap S_1$ will give an adversary the power to correctly decrypt both ciphertexts above. In this case, $m_0 \neq m_1$ is disallowed in order to avoid the trivial attack.

State of the Art. Although anonymity is crucial for BE, it has not received much attentions to construct ANOBE with the proper security guarantee.

In 2006, Barth *et al.* [BBW06] first identified the *anonymity* (i.e., *recipient privacy* in their work) in the context of encrypted file system. They introduced the notion of ANOBE in

the name of *private broadcast encryption*. In their work, two constructions were described. The first one is a generic construction from an IND-CCA secure PKE with key-privacy and a strongly unforgeable signature scheme. They claimed that it achieves IND-CCA security and anonymity but in the *selective* (or static) model which means that the adversary must commit the challenge target sets (S_0, S_1) in advance. Basically, a BE ciphertext there is a set of PKE ciphertexts intended for every recipient in S bound together via a signature. One drawback of this construction is that the decryption time is proportional to $|S|$ since each receiver has to try to decrypt each PKE ciphertext one by one. In their second construction, they introduced a method helping a receiver to find the right PKE ciphertext and reduced the decryption cost to constant. However, it unfortunately relies on the random oracle model.

At PKC 2012, Libert *el al.* [LPQ12] formally revisited Barth *et al.*'s results. They described the *adaptive* security for ANOBE where the adversary can choose the challenge target sets (S_0, S_1) at any time (i.e., the security notation we have reviewed), and showed that it can be achieved from IND-CCA secure PKE (plus strongly secure signatures). Note that this result is quite strong in that the underlying PKE is not necessarily key-private. Moreover, the receiver can decrypt in a constant time. However, the size of ciphertext depends on n, the size of universe. They then demonstrated that Barth *et al.*'s first BE is actually IND-CCA secure and anonymous in an *adaptive* sense and provided an alternative construction from IBE [Sha84,CHK04]. This ANOBE has shorter ciphertext (of size $O(|S|)$) but requires the underlying PKE to be weakly robust [ABN10,Moh10] and key-private, and the decryption cost increases to $O(|S|)$. They also formalized the method helping to reduce the decryption cost in Barth *et al.*'s second construction [BBW06] as *anonymous hint system*, which can be viewed as a variant of extractable hash proof systems [Wee10]. The classical randomness-reuse technique [Kur02,BBS03] was then formally studied to reduce the ciphertext size. Finally, a concrete ANOBE based on the Kurosawa-Desmedt PKE [KD04] was proposed. Having their generic ANOBE, they showed that the Kurosawa-Desmedt PKE can be adapted to be key-private and robust, and also support randomness-reuse technique.

Also at PKC 2012, Fazio and Perera [FP12] proposed an ANOBE scheme with sublinear-size ciphertexts but with a much weaker *outsider-anonymity* where users identified by $S_0 \cap S_1$ are not considered to be malicious. More formally, the adversary is forbidden to get any secret key for $i \in S_0 \cap S_1$. However Barth *et al.*'s early work [BBW06] has actually recognized such an inside attacker as a hazard and illustrated how serious the issue is under a chosen-ciphertext attack. In the end, we want to note that Libert *et al.*'s results [LPQ12] are still the best in the sense that they achieve (1) IND-CCA security, (2) *fully* anonymity and (3) random-oracle-freeness. To our best knowledge, there is no follow-up result with all these features simultaneously even when taking the *identity-based* variant into account (see recent work [HWL+16] for more details).

1.1 Contributions

In this paper, we propose two concrete ANOBE schemes. Both of them are obtained by optimizing an instantiation of Libert *et al.*'s generic construction [LPQ12] with *Cramer-Shoup PKE* [CS98,CS02]. We prove, *from scratch*, that they are secure in the sense of [LPQ12] from the standard k-Linear (k-Lin) assumption and the existence of several other cryptographic primitives (such as strongly unforgeable signature and collision-resistant hash function) .

Although our proposals do not deviate from Libert *et al.*'s generic framework [LPQ12], our new start point and customized security proof allow us to gain shorter ciphertexts and tighter reduction than the concrete instantiation in [LPQ12]. (Recall that it is based on Kurosawa-Desmedt PKE [KD04] and the security result follows the generic construction directly.) A comparison between them is shown in Table 1 where we consider instantiations of our two ANOBE under DDH=1-Lin (or SXDH=1-Lin) assumption[3]. We note that these two instantiations are the most efficient ones.

Table 1. Comparison of our two proposals and the concrete ANOBE from [LPQ12] in terms of ciphertext size and reduction tightness. Table (a) is for the schemes supporting fast decryption while we tolerate linear decryption cost in Table (b). In our comparison, the system has n users and ℓ is the size of target set S. We let $\mathbb{G}$ be a finite group where DDH holds while $\mathbb{G}_1$ denotes the first source group of a bilinear group where SXDH holds. The column "Reduction" shows the security loss.

(a) Comparing our first ANOBE with [LPQ12] plus anonymous hint system.

Scheme	$\lvert ct \rvert$	Reduction
[LPQ12]	$(4\ell+5)\lvert\mathbb{G}\rvert + 2\lvert\mathbb{Z}_p\rvert$	$O(n^3)$
Sec. 3	$(2\ell+5)\lvert\mathbb{G}\rvert + 2\lvert\mathbb{Z}_p\rvert$	$O(1)$

(b) Comparing our second ANOBE with [LPQ12] *without* anonymous hint system.

Scheme	$\lvert ct \rvert$	Reduction
[LPQ12]	$(2\ell+5)\lvert\mathbb{G}\rvert + 2\lvert\mathbb{Z}_p\rvert$	$O(n^3)$
Sec. 4	$(\ell+6)\lvert\mathbb{G}_1\rvert$	$O(1)$

Shorter Ciphertext. Our first ANOBE scheme supports fast decryption. Compared with the concrete ANOBE in [LPQ12] equipped with their DDH-based anonymous hint system[4], our ANOBE can save rougly 50% bandwidth. Our second ANOBE is derived from the first one. We sacrifice fast decryption and peruse shorter ciphertext. Compared with concrete ANOBE in [LPQ12], our second ANOBE works with bilinear groups and roughly saves 50% bandwidth[5]. We highlight that this construction almost touches the lower bound of ciphertext size in an anonymous broadcast encryption [KS12]. It is quite surprising that we start from a less efficient basic PKE scheme but finally achieves better space efficiency. We note that the Cramer-Shoup PKE [CS98,CS02] is indeed less efficient than Kurosawa-Desmedt PKE [KD04], but it permits us to use some customized method to optimize the system.

Tighter Reduction. In [LPQ12], their security reduction suffers from $O(n^3)$ loss where n is the size of the universe. This makes it infeasible for large-scale systems such as aforementioned pay-TV application. In particular, we need to use a larger group to compensate the loss, which of course increases the bandwidth and computation costs. In our work, we prove the security of two ANOBE from basic assumption and only suffer constant security

[3] We assume that (1) the verification key and signature for strongly unforgeable one-time signatures consist of 3 group elements and 2 integers, respectively [Gro06] (see Section 4, [CCS09]); (2) the authenticated encryption with key-binding property has a ciphertext of roughly 2 group elements (see Section 6, [LPQ12]).

[4] The resulting ANOBE will also support fast decryption, here we share the randomness between ANOBE and anonymous hint system.

[5] Here we implement the concrete ANOBE from [LPQ12] using elliptic curve.

loss, which is of both theoretical and practical interest. We argue that the result is non-trivial: A potential solution is to employ an IND-CCA secure PKE with tight reduction for multiple users (like [GHKW16,Hof17]) in Libert *et al.*'s generic construction [LPQ12]. However, the simulator still needs to guess which public keys will be associated with target set which is chosen adversarially and causes significant security loss.

1.2 Technical Overview

Our starting point is an instantiation of Libert *et al.*'s generic construction with Cramer-Shoup PKE [CS98,CS02]. In this overview, we first give this instantiation and describe how to derive our two ANOBE schemes from it.

Starting point. Assume a *prime-order group* $(p, \mathbb{G}, g)$. We let $[a] := g^a \in \mathbb{G}$ for all $a \in \mathbb{Z}_p$ and extend it to matrix over $\mathbb{Z}_p$. Assume $S := \{i_1, \ldots, i_\ell\}$. We can instantiate Libert *et al.*'s construction using Cramer-Shoup PKE under k-Lin assumption as below:

$$\begin{aligned}
\mathsf{mpk} &: \{\ [\mathbf{A}]\ , [\mathbf{A}^\top \mathbf{k}_i], [\mathbf{A}^\top \mathbf{x}_i], [\mathbf{A}^\top \mathbf{y}_i]\ \}_{i\in[n]}, (\mathsf{Gen}_{\mathsf{ots}}, \mathsf{Sig}, \mathsf{Ver}), \mathsf{h} \\
\mathsf{sk}_i &: \mathbf{k}_i, \mathbf{x}_i, \mathbf{y}_i \\
\mathsf{ct}_S &: \{\ [\mathbf{r}^\top \mathbf{A}^\top]\ , [\mathbf{r}^\top \mathbf{A}^\top \mathbf{k}_{i_j}] \cdot m, [\mathbf{r}^\top \mathbf{A}^\top (\mathbf{x}_{i_j} + \alpha \cdot \mathbf{y}_{i_j})]\ \}_{j\in[\ell]}, \mathsf{pk}_{\mathsf{ots}}, \sigma
\end{aligned}$$

where $\mathbf{A} \leftarrow_R \mathbb{Z}_p^{(k+1)\times k}$, $\mathbf{k}_i, \mathbf{x}_i, \mathbf{y}_i \leftarrow_R \mathbb{Z}_p^{k+1}$ for $i \in [n]$ and $\mathbf{r} \leftarrow_R \mathbb{Z}_p^k$. The public parameter mpk is basically n public keys of Cramer-Shoup PKE[6] sharing $[\mathbf{A}]$ which is a common technique in the multi-user setting. The ciphertext for S contains ℓ ciphertexts of Cramer-Shoup PKE with randomness $[\mathbf{r}^\top \mathbf{A}^\top]$ reused as [LPQ12]. Following Libert *et al.*'s suggestion, they are then bound together via a strongly unforgeable signature σ under fresh verification key $\mathsf{pk}_{\mathsf{ots}}$ instead of encrypting $m||\mathsf{pk}_{\mathsf{ots}}$.

The above BE is IND-CCA secure and anonymous according to Libert *et al.*'s generic result. However, we can do better by showing a tighter reduction for this concrete ANOBE. The security loss of Libert *et al.*'s reduction (which is $O(n^3)$) is mainly caused by black-box-reduction to the underlying PKE where the simulation need to guess some information about challenge target set. We prove our security result *from scratch*. In particular, we employ the proof technique for IND-CCA PKE in the multi-user setting [GHKW16,Hof17] but adapt it to our broadcast encryption case. We found that we can now avoid guessing adversary's behavior and also corresponding reduction loss.

Our first ANOBE: Shorter Ciphertext for Fast Decryption. The above instantiation has not been equipped with anonymous hint system [LPQ12], so the decryption cost should be $O(\ell)$. (Recall that, intuitively, an anonymous hint system can help the decryptor to find the right ciphertext component intended for him and avoid $O(\ell)$ factor.) However we observe that $\{[\mathbf{r}^\top \mathbf{A}^\top (\mathbf{x}_{i_j} + \alpha \cdot \mathbf{y}_{i_j})]\}_{j\in[\ell]}$ can serve as the hints for fast decryption. This benefits from the fact that tag α is shared by all users in S. In the decryption procedure, a user with secret

[6] Here we use a direct generalization of Cramer-Shoup PKE under the k-Lin assumption. The original Cramer-Shoup PKE corresponds to the case $k = 1$.

key $\mathbf{k}_i, \mathbf{x}_i, \mathbf{y}_i$ can recover $v = [\mathbf{r}^\top \mathbf{A}^\top (\mathbf{x}_i + \alpha \cdot \mathbf{y}_i)]$ and try to find the index j^* such that $v = [\mathbf{r}^\top \mathbf{A}^\top (\mathbf{x}_{i_{j^*}} + \alpha \cdot \mathbf{y}_{i_{j^*}})]$, which indicates the right ciphertext.

This already saves the bandwidth since we need the DDH-based anonymous hint system in [LPQ12] to upgrade Libert *et al.*'s concrete ANOBE in order to achieve fast decryption. Even with randomness reuse technique, this will introduce $2 \cdot |S|$ additional group elements to the ciphertext. The perspective here is that $\{[\mathbf{r}^\top \mathbf{A}^\top (\mathbf{x}_{i_j} + \alpha \cdot \mathbf{y}_{i_j})]\}_{j \in [\ell]}$ act as crucial components for achieving IND-CCA security and hints for fast decryption at the same time while they are realized separately in Libert *et al.*'s concrete ANOBE.

Our Second ANOBE: Compressing Ciphertext Again. We now ask:

Can we reduce the ciphertext size if we can tolerate slower decryption?

Observe that we have ℓ group elements (i.e., $\{[\mathbf{r}^\top \mathbf{A}^\top (\mathbf{x}_{i_j} + \alpha \cdot \mathbf{y}_{i_j})]\}_{j \in [\ell]}$) for consistency check (which is necessary for IND-CCA security) in our first ANOBE. If we assume that each recipient can correctly guess which part is intended for him/her, we can see that only one of these ℓ elements will be used in the decryption procedure. Therefore a promising idea is to ask all recipients to share the consistency check process. A direct way to do so is to

$$\text{replace} \quad \{[\mathbf{r}^\top \mathbf{A}^\top (\mathbf{x}_{i_j} + \alpha \cdot \mathbf{y}_{i_j})]\}_{j \in [\ell]} \quad \text{with} \quad [\mathbf{r}^\top \mathbf{A}^\top (\mathbf{x} + \alpha \cdot \mathbf{y})]$$

and publish $[\mathbf{A}^\top \mathbf{x}]$ and $[\mathbf{A}^\top \mathbf{y}]$ in mpk. Unfortunately, there is a fatal issue. To do the consistency check, we should give each user $\mathbf{x}$ and $\mathbf{y}$ directly and they will be leaked to an adversary through any corrupted user. This totally breaks the IND-CCA security. We circumvent the difficulty by making the consistency check public using the technique by Kiltz and Wee [KW15]. In particular, we adapt our first ANOBE to $\mathbb{G}_1$ of a pairing group $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$ and

$$\text{replace} \quad [\mathbf{r}^\top \mathbf{A}^\top (\mathbf{x} + \alpha \cdot \mathbf{y})]_1 \quad \text{with} \quad [\mathbf{r}^\top \mathbf{A}^\top (\mathbf{X} + \alpha \cdot \mathbf{Y})]_1$$

where $\mathbf{X}, \mathbf{Y} \leftarrow_R \mathbb{Z}_p^{(k+1)\times(k+1)}$. In the public parameter mpk, we publish

$$([\mathbf{A}^\top \mathbf{X}]_1, [\mathbf{A}^\top \mathbf{Y}]_1) \quad \text{and} \quad ([\mathbf{B}]_2, [\mathbf{X}\mathbf{B}]_2, [\mathbf{Y}\mathbf{B}]_2)$$

where $\mathbf{B} \leftarrow_R \mathbb{Z}_p^{(k+1)\times k}$ and the right-hand side part allow *anyone* to *publicly* check the ciphertext consistency.

We have successfully compressed the ciphertext but lose the correctness of decryption since we do not have hint system now. It is easy to fix using *key-binding* symmetric encryption scheme (E, D). That is we pick session key K from the key space of (E, D) and

$$\text{replace} \quad [\mathbf{r}^\top \mathbf{A}^\top \mathbf{k}_{i_j}]_1 \cdot m \quad \text{with} \quad [\mathbf{r}^\top \mathbf{A}^\top \mathbf{k}_{i_j}]_1 \cdot \mathsf{K}, \mathsf{E}_\mathsf{K}(m).$$

We note that we are not pursuing fast decryption now. We can further get rid of σ by defining α as in Cramer-Shoup PKE [CS98,CS02]. We sketch our second ANOBE as follows:

$$\mathsf{mpk} : (\mathsf{E}, \mathsf{D}), \mathsf{h};\ \{\ [\mathbf{A}^\top]_1\ , [\mathbf{A}^\top \mathbf{k}_i]_1,\ [\mathbf{A}^\top \mathbf{X}]_1, [\mathbf{A}^\top \mathbf{Y}]_1\ \}_{i \in [n]};\ [\mathbf{B}]_2, [\mathbf{X}\mathbf{B}]_2, [\mathbf{Y}\mathbf{B}]_2$$

$$\mathsf{sk}_i : \mathbf{k}_i$$

$$\mathsf{ct}_S : \{\ [\mathbf{r}^\top \mathbf{A}^\top]_1\ , [\mathbf{r}^\top \mathbf{A}^\top \mathbf{k}_{i_j}]_1 \cdot \mathsf{K},\ \mathsf{E}_\mathsf{K}(m)\ ,\ [\mathbf{r}^\top \mathbf{A}^\top (\mathbf{X} + \alpha \cdot \mathbf{Y})]_1\ \}_{j \in [\ell]}$$

where all terms in gray box are shared by all users/receivers. As our first ANOBE, the reduction loss is constant.

Compared with Libert *et al.*'s concrete ANOBE [LPQ12], our second ANOBE is based on weaker assumptions — we don't require the existence of strongly one-time signature and (E, D) is not necessarily authenticated encryption. Furthermore, in the ciphertext, we share as many components as possible among receivers in the target set, the remaining ℓ group elements seem to be inevitable by the lower bound [KS12].

Organization. Our paper is organized as follows. We review some basic notions in Section 2. Our two ANOBE constructions along with security analysis will be presented in Section 3 and Section 4, respectively. We finally conclude the paper in Section 5.

2 Preliminaries

Notations. For $n \in \mathbb{N}$, we define $[n] := \{1, 2, \ldots, n\}$. We use $a \leftarrow_R A$ to denote the process of uniformly sampling an element from set A and assigning it to variable a. For two sets S_0, S_1, define $S_0 \triangle S_1 := (S_0 \setminus S_1) \cup (S_1 \setminus S_0)$. "p.p.t." stands for probabilistic polynomial time.

2.1 Anonymous Broadcast Encryption

Algorithms. Let $\mathcal{U} := [n]$ be the universe. A *broadcast encryption* (BE) scheme consists of four algorithms $(\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$:

- $\mathsf{Setup}(1^\lambda, n) \to (\mathsf{mpk}, \mathsf{msk})$: on input 1^λ and n, the *setup algorithm* outputs a master public key mpk and a master secret key msk.
- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, i) \to \mathsf{sk}_i$: on input mpk, msk and an index $i \in \mathcal{U}$, the *key generation algorithm* outputs a secret key sk_i.
- $\mathsf{Enc}(\mathsf{mpk}, m, S) \to \mathsf{ct}_S$: on input mpk, a message m and a subset $S \subseteq \mathcal{U}$, the *encryption algorithm* outputs a ciphertext ct_S.
- $\mathsf{Dec}(\mathsf{mpk}, \mathsf{ct}_S, \mathsf{sk}_i) \to m/\perp$: on input mpk, ct_S and sk_i, the *decryption algorithm* outputs m or a failure symbol $\perp$.

Correctness. For all λ, all $(\mathsf{mpk}, \mathsf{msk}) \leftarrow_R \mathsf{Setup}(1^\lambda, n)$, all m, all $S \subseteq \mathcal{U}$, and all $i \in S$, it is required that $\mathsf{Dec}(\mathsf{mpk}, \mathsf{Enc}(\mathsf{mpk}, m, S), \mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, i)) = m$.

Chosen-ciphertext security and anonymity. For any adversary $\mathcal{A}$, define

$$\mathsf{Adv}^{\mathsf{BE}}_{\mathcal{A}}(1^\lambda) := \left| \Pr \left[b = b' \;\middle|\; \begin{array}{c} (\mathsf{mpk}, \mathsf{msk}) \leftarrow_R \mathsf{Setup}(1^\lambda, n),\ b \leftarrow_R \{0,1\} \\ (m_0, m_1, S_0, S_1) \leftarrow_R \mathcal{A}^{\mathsf{KeyO}(\cdot), \mathsf{DecO}(\cdot,\cdot)}(1^\lambda, \mathsf{mpk}) \\ \mathsf{ct}^* \leftarrow_R \mathsf{Enc}(\mathsf{mpk}, m_b, S_b) \\ b' \leftarrow_R \mathcal{A}^{\mathsf{KeyO}(\cdot), \mathsf{DecO}(\cdot,\cdot)}(1^\lambda, \mathsf{mpk}, \mathsf{ct}^*) \end{array} \right] - \frac{1}{2} \right|$$

where oracles work as follows:

– KeyO: on input i, *key extraction oracle* KeyO outputs $\mathsf{sk}_i \leftarrow_R \mathsf{KeyGen}(\mathsf{msk}, \mathsf{mpk}, i)$ and sets $Q_{\mathsf{sk}} := Q_{\mathsf{sk}} \cup \{i\}$ which is initialized to be $\emptyset$ at the beginning.
– DecO: on input (ct, i), *decryption oracle* DecO outputs $\mathsf{Dec}(\mathsf{mpk}, \mathsf{ct}, \mathsf{sk}_i)$ when ct^* (a.k.a. *challenge ciphertext*) has not been defined or $\mathsf{ct} \neq \mathsf{ct}^*$.

A broadcast encryption scheme achieves chosen-ciphertext security and anonymity (ANO-IND-CCA) if, for all p.p.t. adversary $\mathcal{A}$, $\mathsf{Adv}^{\mathsf{BE}}_{\mathcal{A}}(\lambda)$ is negligible in λ under the restrictions that (1) $|m_0| = |m_1|$ and $|S_0| = |S_1|$; (2) $Q_{\mathsf{sk}} \cap (S_0 \triangle S_1) = \emptyset$; (3) if $Q_{\mathsf{sk}} \cap (S_0 \cap S_1) \neq \emptyset$, then $m_0 = m_1$.

2.2 Prime-Order (Bilinear) Groups

Prime-order group. A group generator GGen is a p.p.t. algorithm which takes 1^λ as input and outputs a description $\mathcal{G} := (p, \mathbb{G}, g)$. Here $\mathbb{G}$ is a finite cyclic group of prime order p and g is a random generator of $\mathbb{G}$. Throughout the paper, we will use *implicit representation* [EHK+13]. We let $[a] := g^a \in \mathbb{G}$ for all $a \in \mathbb{Z}_p$. For a matrix $\mathbf{A} = (a_{ij}) \in \mathbb{Z}_p^{m \times n}$, we let $[\mathbf{A}] = (g^{a_{ij}}) \in \mathbb{G}^{m \times n}$.

Prime-order bilinear group. A group generator PGGen is a p.p.t. algorithm which takes 1^λ as input and outputs a description $\mathcal{PG} := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2)$ of (asymmetric) bilinear group. Here $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ are finite cyclic groups of prime order p and e is an admissible bilinear map. $g_1 \in \mathbb{G}_1$ and $g_2 \in \mathbb{G}_2$ are random generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, and $g_T := e(g_1, g_2)$ will be a generator of group $\mathbb{G}_T$. The implicit representation is also be applied to prime-order *bilinear* groups: We let $[a]_s := g_s^a \in \mathbb{G}_s$ for all $a \in \mathbb{Z}_p$ and $s \in \{1, 2, T\}$. The notation can be easily extended to matrices analogously and we let $e([\mathbf{A}]_1, [\mathbf{B}]_2) := [\mathbf{AB}]_T$ for matrices $\mathbf{A}$ and $\mathbf{B}$ when the multiplication is well-defined.

Cryptographic assumption. For any $k \in \mathbb{N}$, we call $\mathcal{D}_k$ a *matrix distribution* if it outputs full-rank matrices in $\mathbb{Z}_p^{(k+1)\times k}$ in polynomial time. We may assume that for all $\mathbf{A} \leftarrow_R \mathcal{D}_k$, the first k rows of $\mathbf{A}$ form an invertible matrix.

We will use the $\mathcal{D}_k$-Matrix Diffie-Hellman ($\mathcal{D}_k$-MDDH) assumption in $\mathbb{G}$ described as follows. The $\mathcal{D}_k$-MDDH assumption in $\mathbb{G}_1$ and $\mathbb{G}_2$ are analogous.

Assumption 1 ($\mathcal{D}_k$-MDDH) *We say that the $\mathcal{D}_k$-Matrix Diffie-Hellman assumption holds relative to GGen, if for any p.p.t. adversary $\mathcal{A}$, the following advantage function is negligible in λ.*

$$\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{A},\mathbb{G}}(\lambda) := |\Pr[\mathcal{A}(\mathcal{G}, [\mathbf{A}], [\mathbf{As}]) = 1] - \Pr[\mathcal{A}(\mathcal{G}, [\mathbf{A}], [\mathbf{u}]) = 1]|$$

where $\mathcal{G} \leftarrow_R \mathsf{GGen}(1^\lambda)$, $\mathbf{A} \leftarrow_R \mathcal{D}_k$, $\mathbf{s} \leftarrow_R \mathbb{Z}_p^k$, and $\mathbf{u} \leftarrow_R \mathbb{Z}_p^{k+1}$.

The famous k-Linear (k-Lin) assumption is an instantiation of the $\mathcal{D}_k$-MDDH assumption. The classical *decisional Diffie-Hellman* (DDH) assumption (a.k.a *symmetric external Diffie-Hellman* (SXDH) assumption in *asymmetric* bilinear groups) is just the k-Lin assumption with $k = 1$. See [EHK+13] for more details.

For bilinear groups, we also use the $\mathcal{D}_k$-Matrix Kernel Diffie-Hellman ($\mathcal{D}_k$-KerMDH) Assumption [MRV16], which is implied by the $\mathcal{D}_k$-MDDH assumption.

Assumption 2 ($\mathcal{D}_k$-KerMDH) *Let $s \in \{1,2\}$. We say that the $\mathcal{D}_k$-Kernel Matrix Diffie-Hellman Assumption holds relative to* PGGen*, if for any p.p.t. adversary $\mathcal{A}$, the following advantage function is negligible in λ.*

$$\mathsf{Adv}^{\mathsf{kmdh}}_{\mathcal{A},\mathcal{G}_s}(\lambda) := \Pr[\mathbf{A}^\top \mathbf{a}^\perp = \mathbf{0} \wedge \mathbf{a}^\perp \neq \mathbf{0} \mid [\mathbf{a}^\perp]_{3-s} \leftarrow_R \mathcal{A}(\mathcal{PG}, [\mathbf{A}]_s)]$$

where $\mathcal{PG} \leftarrow_R \mathsf{PGGen}(1^\lambda)$, $\mathbf{A} \leftarrow_R \mathcal{D}_k$.

2.3 Cryptographic Primitives

Our constructions will use the following cryptographic primitives:

Key-binding secure symmetric encryption. A symmetric encryption scheme with a key space $\mathcal{K}$ consists of two algorithms (E, D):

- $\mathsf{E}_K(m) \to c$: the *encryption algorithm* generates a encryption c of the message m under the secret key K.
- $\mathsf{D}_K(c) \to m/\perp$: the *decryption algorithm* decrypts the ciphertext c using K, and returns m or a failure symbol $\perp$.

The correctness can be stated as follows: for all $K \leftarrow_R \mathcal{K}$ and all message m, we have $\mathsf{D}_K(\mathsf{E}_K(m)) = m$ with overwhelming probability. We then review the semantic security of symmetric encryptions. For any adversary $\mathcal{A}$, define

$$\mathsf{Adv}^{\mathsf{se}}_{\mathcal{A}}(\lambda) := \left| \Pr\left[b = b' \;\middle|\; \begin{array}{c} (m_0, m_1) \leftarrow_R \mathcal{A}(1^\lambda, \mathcal{K}) \\ K \leftarrow_R \mathcal{K},\ b \leftarrow_R \{0,1\},\ c^* \leftarrow_R \mathsf{E}_K(m_b) \\ b' \leftarrow_R \mathcal{A}(1^\lambda, \mathcal{K}, c^*) \end{array} \right] - \frac{1}{2} \right|.$$

A symmetric encryption is *semantically secure*, if for all p.p.t. adversary $\mathcal{A}$, the advantage function $\mathsf{Adv}^{\mathsf{se}}_{\mathcal{A}}(\lambda)$ is negligible in λ.

Furthermore, we require the symmetric encryption to be *key-binding* [Fis99]. Namely, for any message m and any secret key $K \in \mathcal{K}$, there exists no key $K' \in \mathcal{K}$ such that $K \neq K'$ and $\mathsf{D}_{K'}(\mathsf{E}_K(m)) \neq \perp$. See [Fis99] for more details.

Collision-resilient hash function. A family of hash functions $\mathcal{H}$ is said to be *collision-resistant* if, for all p.p.t. algorithm $\mathcal{A}$, the following advantage function is negligible in λ.

$$\mathsf{Adv}^{\mathsf{hash}}_{\mathcal{A}}(\lambda) := \Pr[h(x) = h(y) \wedge x \neq y \mid h \leftarrow_R \mathcal{H}, (x,y) \leftarrow_R \mathcal{A}(1^\lambda, h)].$$

Strongly secure one-time signature. A *signature* scheme consists of the following three algorithms.

- $\mathsf{Gen}_{\mathsf{ots}}(1^\lambda) \to (\mathsf{sk}_{\mathsf{ots}}, \mathsf{pk}_{\mathsf{ots}})$: on input the security parameter λ, the *key generation algorithm* outputs a signing key $\mathsf{sk}_{\mathsf{ots}}$ and the verification key $\mathsf{pk}_{\mathsf{ots}}$.
- $\mathsf{Sign}(\mathsf{sk}_{\mathsf{ots}}, m) \to \sigma$: on input $\mathsf{sk}_{\mathsf{ots}}$ and a message m, the *signing algorithm* outputs a signature σ.

– $\mathsf{Ver}(\mathsf{pk}_{\mathsf{ots}}, m, \sigma) \to 0/1$: on input $\mathsf{pk}_{\mathsf{ots}}, m,$ and σ, the *verification algorithm* outputs 0 (reject) or 1 (accept).

We require the signature scheme *strongly unforgeable* against all adversaries with *at most one* message-signature pair. Formally, for any adversary $\mathcal{A}$, we define

$$\mathsf{Adv}^{\mathsf{ots}}_{\mathcal{A}}(\lambda) := \left| \Pr \left[\begin{array}{l|c} \mathsf{Ver}(\mathsf{pk}_{\mathsf{ots}}, m^*, \sigma^*) = 1 & (\mathsf{sk}_{\mathsf{ots}}, \mathsf{pk}_{\mathsf{ots}}) \leftarrow_{\mathrm{R}} \mathsf{Gen}_{\mathsf{ots}}(1^\lambda) \\ \wedge\, (m, \sigma) \neq (m^*, \sigma^*) & (m^*, \sigma^*) \leftarrow_{\mathrm{R}} \mathcal{A}^{\mathsf{SigO}(\cdot)}(1^\lambda, \mathsf{pk}_{\mathsf{ots}}) \end{array} \right] - \frac{1}{2} \right|,$$

where the oracle SigO takes m as input and returns $\sigma \leftarrow_{\mathrm{R}} \mathsf{Sign}(\mathsf{sk}_{\mathsf{ots}}, m)$, and can only be called *once*. We say that a signature scheme is *strongly unforgeable under one-time chosen message attack* if the advantage function $\mathsf{Adv}^{\mathsf{ots}}_{\mathcal{A}}(\lambda)$ is negligible in λ for all p.p.t. adversary $\mathcal{A}$.

2.4 Core Lemma

We review the core lemma in [KW15].

Lemma 1 (Core lemma, [KW15]). *Let $k \in \mathbb{N}$. For any $\mathbf{A}, \mathbf{B} \in \mathbb{Z}_p^{(k+1)\times k}$ and any (possibly unbounded) adversary $\mathcal{A}$, we have*

$$\Pr \left[\begin{array}{l|c} \mathbf{u} \notin \mathsf{span}(\mathbf{A}) \wedge \alpha \neq \alpha^* & \mathbf{X}, \mathbf{Y} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{(k+1)\times(k+1)} \\ \wedge\, \boldsymbol{\pi}^\top = \mathbf{u}^\top(\mathbf{X} + \alpha \cdot \mathbf{Y}) & (\mathbf{u}, \alpha, \boldsymbol{\pi}) \leftarrow_{\mathrm{R}} \mathcal{A}^{\mathcal{O}(\cdot)}(\mathbf{A}^\top\mathbf{X}, \mathbf{A}^\top\mathbf{Y}, \mathbf{XB}, \mathbf{YB}) \end{array} \right] \leqslant \frac{1}{p}$$

where $\mathcal{O}(\alpha^*) \to \mathbf{X} + \alpha^* \cdot \mathbf{Y}$ may only be called one time.

3 Tightly Secure ANOBE with Fast Decryption

3.1 Construction

Our first broadcast encryption scheme is described as follows.

– $\mathsf{Setup}(1^\lambda, n)$: Run $\mathcal{G} := (p, \mathbb{G}, g) \leftarrow_{\mathrm{R}} \mathsf{GGen}(1^\lambda)$. Sample

$$\mathbf{A} \leftarrow_{\mathrm{R}} \mathcal{D}_k \quad \text{and} \quad \mathbf{k}_i, \mathbf{x}_i, \mathbf{y}_i \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1} \ \text{ for } \ i \in [n].$$

Select a strongly unforgeable one-time signature scheme $(\mathsf{Gen}_{\mathsf{ots}}, \mathsf{Sig}, \mathsf{Ver})$ and a hash function $\mathsf{h} : \{0,1\}^* \to \mathbb{Z}_p$ from $\mathcal{H}$. The master public key is

$$\mathsf{mpk} := (\mathcal{G}, \mathsf{h}, (\mathsf{Gen}_{\mathsf{ots}}, \mathsf{Sig}, \mathsf{Ver}), [\mathbf{A}], \{[\mathbf{A}^\top\mathbf{k}_i], [\mathbf{A}^\top\mathbf{x}_i], [\mathbf{A}^\top\mathbf{y}_i]\}_{i=1}^n)$$

and the master secret key is $\mathsf{msk} := (\{\mathbf{k}_i, \mathbf{x}_i, \mathbf{y}_i\}_{i=1}^n)$.

– $\mathsf{KeyGen}(\mathsf{msk}, \mathsf{mpk}, i)$: Output the secret key $\mathsf{sk}_i = (\mathbf{k}_i, \mathbf{x}_i, \mathbf{y}_i)$.

– $\mathsf{Enc}(\mathsf{mpk}, m, S)$: Let $\ell := |S|$ and $S = \{i_1, \ldots, i_\ell\} \subseteq \mathsf{U} = [n]$. Sample $\mathbf{r} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$ and compute

$$[\mathbf{u}^\top] := [\mathbf{r}^\top\mathbf{A}^\top].$$

Generate $(\mathsf{sk}_{\mathsf{ots}}, \mathsf{pk}_{\mathsf{ots}}) \leftarrow_R \mathsf{Gen}_{\mathsf{ots}}(1^\lambda)$, compute $\alpha := \mathsf{h}(\mathsf{pk}_{\mathsf{ots}})$ and

$$\begin{aligned} c_1 &:= [\mathbf{r}^\top \mathbf{A}^\top \mathbf{k}_{i_1}] \cdot m, \nu_1 := [\mathbf{r}^\top \mathbf{A}^\top (\mathbf{x}_{i_1} + \alpha \cdot \mathbf{y}_{i_1})], \\ &\vdots \qquad\qquad\qquad\qquad \vdots \\ c_\ell &:= [\mathbf{r}^\top \mathbf{A}^\top \mathbf{k}_{i_\ell}] \cdot m, \nu_\ell := [\mathbf{r}^\top \mathbf{A}^\top (\mathbf{x}_{i_\ell} + \alpha \cdot \mathbf{y}_{i_\ell})]. \end{aligned}$$

Choose a random permutation τ over $[\ell]$ and compute

$$\sigma := \mathsf{Sig}(\mathsf{sk}_{\mathsf{ots}}, ([\mathbf{u}^\top], c_{\tau(1)}, \nu_{\tau(1)}, \ldots, c_{\tau(\ell)}, \nu_{\tau(\ell)})).$$

The ciphertext is

$$\mathsf{ct} := ([\mathbf{u}^\top], c_{\tau(1)}, \nu_{\tau(1)}, \ldots, c_{\tau(\ell)}, \nu_{\tau(\ell)}, \mathsf{pk}_{\mathsf{ots}}, \sigma).$$

– $\mathsf{Dec}(\mathsf{mpk}, \mathsf{ct}, \mathsf{sk}_i)$: Parse the ciphertext ct as $([\mathbf{u}^\top], \bar{c}_1, \bar{\nu}_1, \ldots, \bar{c}_\ell, \bar{\nu}_\ell, \mathsf{pk}_{\mathsf{ots}}, \sigma)$ and the secret key sk_i as $(\mathbf{k}_i, \mathbf{x}_i, \mathbf{y}_i)$. Return $\perp$ if

$$\mathsf{Ver}(\mathsf{pk}_{\mathsf{ots}}, ([\mathbf{u}^\top], \bar{c}_1, \bar{\nu}_1, \ldots, \bar{c}_\ell, \bar{\nu}_\ell), \sigma) = 0,$$

otherwise, compute

$$\nu := [\mathbf{u}^\top (\mathbf{x}_i + \alpha \cdot \mathbf{y}_i)],$$

where $\alpha = \mathsf{h}(\mathsf{pk}_{\mathsf{ots}})$. If there exists $j \in [\ell]$ such that $\nu = \bar{\nu}_j$, return $m' := \bar{c}_j / [\mathbf{u}^\top \mathbf{k}_i]$; otherwise, return $\perp$.

Correctness. For any ciphertext $\mathsf{ct} = ([\mathbf{u}^\top], \bar{c}_1, \bar{\nu}_1, \ldots, \bar{c}_\ell, \bar{\nu}_\ell, \mathsf{pk}_{\mathsf{ots}}, \sigma)$ for set $S \subseteq \mathcal{U}$ generated by Enc, we always have

$$\mathsf{Ver}(\mathsf{pk}_{\mathsf{ots}}, ([\mathbf{u}^\top], \bar{c}_1, \bar{\nu}_1, \ldots, \bar{c}_\ell, \bar{\nu}_\ell), \sigma) = 1$$

by the correctness of signature scheme $(\mathsf{Gen}_{\mathsf{ots}}, \mathsf{Sig}, \mathsf{Ver})$. Given secret key $\mathsf{sk}_i = (\mathbf{k}_i, \mathbf{x}_i, \mathbf{y}_i)$ for $i \in S$, there must exist an index $j \in [\ell]$ such that

$$\nu = [\mathbf{u}^\top (\mathbf{x}_i + \alpha \cdot \mathbf{y}_i)] = \bar{\nu}_j,$$

and then it is not hard to see that the message can be recovered from $\bar{c}_j$.

3.2 Security Result and Proof Overview

We prove the following theorem.

Theorem 1 *Our broadcast encryption scheme in Section 3.1 is adaptively ANO-IND-CCA secure assuming that: (1) $\mathcal{H}$ is collision-resistant; (2) the $\mathcal{D}_k$-MDDH assumption holds in $\mathbb{G}$; (3) signature scheme $(\mathsf{Gen}_{\mathsf{ots}}, \mathsf{Sig}, \mathsf{Ver})$ is strongly unforgeable under one-time chosen message attack. Concretely, for any adversary $\mathcal{A}$, there exist algorithms $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$ such that*

$$\mathsf{Adv}^{\mathsf{BE}}_{\mathcal{A}}(\lambda) \leqslant \mathsf{Adv}^{\mathsf{mddh}}_{\mathbb{G},\mathcal{B}_1}(\lambda) + \mathsf{Adv}^{\mathsf{ots}}_{\mathcal{B}_2}(\lambda) + \mathsf{Adv}^{\mathsf{hash}}_{\mathcal{B}_3}(\lambda) + O(1/p)$$

and $\mathsf{Time}(\mathcal{B}_1), \mathsf{Time}(\mathcal{B}_2), \mathsf{Time}(\mathcal{B}_3) \approx \mathsf{Time}(\mathcal{A})$.

We prove the theorem via the following game sequence.

Game_0. This game is identical to the real game described in Section 2.1. In particular, our simulation is as follows:

Setup. Run $\mathsf{Setup}(1^\lambda, n)$ and send $\mathcal{A}$ the master public key

$$\mathsf{mpk} := (\mathcal{G}, h, (\mathsf{Gen}_{\mathsf{ots}}, \mathsf{Sig}, \mathsf{Ver}), [\mathbf{A}], \{[\mathbf{A}^\top \mathbf{k}_i], [\mathbf{A}^\top \mathbf{x}_i], [\mathbf{A}^\top \mathbf{y}_i]\}_{i=1}^n)$$

and keep the master secret key $\mathsf{msk} := (\{\mathbf{k}_i, \mathbf{x}_i, \mathbf{y}_i\}_{i=1}^n)$. Set $Q_{\mathsf{sk}} := \emptyset$.

Challenge ciphertext. Receiving (m_0, m_1, S_0, S_1) from $\mathcal{A}$ where we let $S_0 = \{i_{1,0}, \ldots, i_{\ell,0}\}$ and $S_1 = \{i_{1,1}, \ldots, i_{\ell,1}\}$, pick $b \leftarrow_R \{0,1\}$, $\mathbf{u}^* \leftarrow_R \mathsf{span}(\mathbf{A})$, $(\mathsf{sk}^*_{\mathsf{ots}}, \mathsf{pk}^*_{\mathsf{ots}}) \leftarrow_R \mathsf{Gen}_{\mathsf{ots}}(1^\lambda)$, choose a random permutation τ over $[\ell]$, let $\alpha^* = h(\mathsf{pk}^*_{\mathsf{ots}})$ and compute

$$\mathsf{ct}^*_1 := ([\mathbf{u}^{*\top}], c^*_1, v^*_1, \ldots, c^*_\ell, v^*_\ell)$$

where $c^*_j = [\mathbf{u}^{*\top} \mathbf{k}_{i_{\tau(j),b}}] \cdot m_b$ and $v^*_j = [\mathbf{u}^{*\top}(\mathbf{x}_{i_{\tau(j),b}} + \alpha^* \cdot \mathbf{y}_{i_{\tau(j),b}})]$ for $j \in [\ell]$. Output the challenge ciphertext

$$\mathsf{ct}^* := (\mathsf{ct}^*_1, \mathsf{pk}^*_{\mathsf{ots}}, \sigma^* := \mathsf{Sig}(\mathsf{sk}^*_{\mathsf{ots}}, \mathsf{ct}^*_1)).$$

Simulating KeyO. On input $i \in U$, output $\mathsf{sk}_i = (\mathbf{k}_i, \mathbf{x}_i, \mathbf{y}_i)$ and update $Q_{\mathsf{sk}} := Q_{\mathsf{sk}} \cup \{i\}$.

Simulating DecO. On input (ct, i), parse

$$\mathsf{ct} = (\mathsf{ct}_1 = ([\mathbf{u}^\top], c_1, v_1, \ldots, c_\ell, v_\ell), \mathsf{pk}_{\mathsf{ots}}, \sigma),$$

reject the query if

$$(a) \quad \mathsf{ct} = \mathsf{ct}^*$$

$$\text{or} \quad (b) \quad \mathsf{Ver}(\mathsf{pk}_{\mathsf{ots}}, \mathsf{ct}_1, \sigma) = 0.$$

Then compute $\alpha = h(\mathsf{pk}_{\mathsf{ots}})$ and $v = [\mathbf{u}^\top(\mathbf{x}_i + \alpha \cdot \mathbf{y}_i)]$. If there exists $j \in [\ell]$ such that $v = v_j$, return $m' := c_j / [\mathbf{u}^\top \mathbf{k}_i]$; otherwise, return $\perp$.

Finalize. Received b' from $\mathcal{A}$, return 1 if $b = b'$; otherwise return 0.

Let Win_i denote the event that $\mathcal{A}$ in Game_i guesses b correctly. Since Game_0 perfectly simulates the real game, we have $\mathsf{Adv}^{\mathsf{BE}}_{\mathcal{A}}(1^\lambda) = |\Pr[\mathsf{Win}_0] - 1/2|$.

Game_1. This game is identical to Game_0 except that we sample $\mathbf{u}^* \leftarrow_R \mathbb{Z}_p^{k+1}$ when generating the challenge ciphertext ct^*. It is easy to see that this game is indistinguishable from Game_0 under the $\mathcal{D}_k$-MDDH assumption. Formally, we have the following lemma.

Lemma 2 ($\mathsf{Game}_1 \approx_c \mathsf{Game}_0$). *There exists an adversary $\mathcal{B}_1$ such that*

$$|\Pr[\mathsf{Win}_1] - \Pr[\mathsf{Win}_0]| \leqslant \mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{G},\mathcal{B}_1}(\lambda).$$

Game_2. This game is identical to Game_1 except that DecO, on input (ct, i), rejects the query if (a) or (b) or

$$(c) \quad \mathsf{pk}_{\mathsf{ots}} = \mathsf{pk}^*_{\mathsf{ots}}.$$

This game is identical to Game_1 until $\mathcal{A}$ submits a query with $\mathsf{pk}_{\mathsf{ots}} = \mathsf{pk}^*_{\mathsf{ots}}$ which survives under condition (a) and (b). However σ in such a query will violate the strong unforgeability of $(\mathsf{Gen}_{\mathsf{ots}}, \mathsf{Sig}, \mathsf{Ver})$, and this game is indistinguishable from Game_1. Formally, we have the following lemma.

Lemma 3 **($\mathsf{Game}_2 \approx_c \mathsf{Game}_1$).** *There exists an adversary $\mathcal{B}_2$ such that*

$$|\Pr[\mathsf{Win}_2] - \Pr[\mathsf{Win}_1]| \leqslant \mathsf{Adv}^{\mathsf{ots}}_{\mathcal{B}_2}(\lambda).$$

Game_3**.** This game is identical to Game_2 except the following substitution:

$$(c) \quad \mathsf{pk}_{\mathsf{ots}} = \mathsf{pk}^*_{\mathsf{ots}} \quad \longmapsto \quad (c') \quad \alpha = \alpha^*$$

This game is identical to Game_2 until $\mathcal{A}$ submits a query with $\mathsf{pk}_{\mathsf{ots}} \neq \mathsf{pk}^*_{\mathsf{ots}}$ but $\alpha = \alpha^*$. This immediately violates the collision-resistance of $\mathcal{H}$, and this game is indistinguishable from Game_2. Formally, we have the following lemma.

Lemma 4 **($\mathsf{Game}_3 \approx_c \mathsf{Game}_2$).** *There exists an algorithm $\mathcal{B}_3$ such that*

$$|\Pr[\mathsf{Win}_3] - \Pr[\mathsf{Win}_2]| \leqslant \mathsf{Adv}^{\mathsf{hash}}_{\mathcal{B}_3}(\lambda).$$

Game_4**.** This game is identical to Game_3 except that except that DecO, on input (ct, i), rejects the query if (a) or (b) or (c') or

$$(d) \quad \mathbf{u} \notin \mathsf{span}(\mathbf{A})$$

We have the following lemma stating that this game is statistically indistinguishable with Game_3.

Lemma 5 **($\mathsf{Game}_4 \approx_s \mathsf{Game}_3$).** $|\mathsf{Win}_4 - \mathsf{Win}_3| \leqslant O(1/p)$.

Let q_D be the number of decryption queries. The lemma can be proved in q_D steps. In the j-th step, assuming that the first $j-1$ decryption queries have been processed with condition (d), we demonstrate that the j-th query will finally be rejected if it survives under condition $(a), (b), (c')$ with $\mathbf{u} \notin \mathsf{span}(\mathbf{A})$. In other words, we can introduce condition (d) here without changing adversary's view. The proof (for the j-th step) relies on the observation that we leak no more information than $\{\mathbf{A}^\top \mathbf{x}_\eta, \mathbf{A}^\top \mathbf{y}_\eta\}_{\eta \in [n]}$ when answering the first $j-1$ queries to DecO. With the help of condition (c'), which ensures that $\alpha \neq \alpha^*$, we can claim that $\mathbf{u}^\top(\mathbf{x}_i + \alpha \cdot \mathbf{y}_i)$ is independently and uniformly distributed and thus hard to guess.

Finally, we have the following lemma which proves Theorem 1 when combining with all previous lemmas and claims.

Lemma 6. $\Pr[\mathsf{Win}_4] = 1/2$.

This follows from the fact that $(\mathbf{u}^*\mathbf{k}_i, \mathbf{u}^*(\mathbf{x}_i + \alpha \cdot \mathbf{y}_i))$ are uniformly distributed over $\mathbb{G}^2$, especially unrelated to b, for all $i \in S_b$ (resp. $i \in S_b/S_{1-b}$) when $Q_{\mathsf{sk}} \cap (S_0 \cap S_1) = \emptyset$ (resp. $Q_{\mathsf{sk}} \cap (S_0 \cap S_1) \neq \emptyset$), conditioned on mpk, KeyO and DecO. The analysis is similar to that for Lemma 5.

Perspective. Lemma 5 and Lemma 6 are at the core of our proof. Although our proofs still rely on the proof technique of underlying Cramer-Shoup PKE, we get rid of large reduction loss by carrying out the argument in the broadcast setting *directly*. In particular, we employ the technique beneath the core lemma from Kiltz and Wee [KW15] (see Lemma 1), which allows us to take *all* users into account in a *non-adaptive* way first and then upgrade to the adaptive setting for free. This avoids guessing adversary's behaviour in the simulation which caused large security loss in Libert *et al.*'s work [LPQ12]. Furthermore, we note that our proof indeed involves *robustness* [ABN10,Moh10,LPQ12] but in an *implicit* manner since we are not working with generic PKE anymore.

3.3 Omitted Proofs

Proof of Lemma 3: In Game_2, let Forge denote the event that $\mathcal{A}$ submits a query with $\mathsf{ct} := (\mathsf{ct}_1, \mathsf{pk}_{\mathsf{ots}} = \mathsf{pk}^*_{\mathsf{ots}}, \sigma)$ to DecO which can not be rejected by condition $(\mathfrak{a})$ and $(\mathfrak{b})$. Observe that Game_2 is identical to Game_1 if Forge does not happen, we have

$$|\Pr[\mathsf{Win}_2] - \Pr[\mathsf{Win}_1]| \leqslant \Pr[\mathsf{Forge}].$$

We bound $\Pr[\mathsf{Forge}]$ via the following reduction. On input $\mathsf{pk}^*_{\mathsf{ots}}$, algorithm $\mathcal{B}_2$ prepares mpk and simulates $\mathsf{KeyO}, \mathsf{DecO}$ honestly as in Game_2. When generating the challenge ciphertext, it generates ct^*_1 as in Game_2 and output $\mathsf{ct}^* := (\mathsf{ct}^*_1, \mathsf{pk}^*_{\mathsf{ots}}, \sigma^*)$, where σ^* is obtained from the SigO with input ct^*_1. Once Forge happens when answering query with $(\mathsf{ct}_1, \mathsf{pk}_{\mathsf{ots}} = \mathsf{pk}^*_{\mathsf{ots}}, \sigma)$, $\mathcal{B}_2$ outputs (ct_1, σ). The condition $(\mathfrak{b})$ ensure that σ is valid signature and condition $(\mathfrak{a})$ ensure that $(\mathsf{ct}_1, \sigma) \neq (\mathsf{ct}^*_1, \sigma^*)$. This readily proves the lemma. □

Proof of Lemma 4: In Game_3, let Coll be the event that $\mathcal{A}$ submits a query with $\mathsf{ct} := (\mathsf{ct}_1, \mathsf{pk}_{\mathsf{ots}}, \sigma)$ to DecO such that $\mathsf{pk}_{\mathsf{ots}} \neq \mathsf{pk}^*_{\mathsf{ots}}$ but $\alpha = \alpha^*$. Observe that Game_3 is identical to Game_2 if Coll does not happen. That is we have

$$|\Pr[\mathsf{Win}_3] - \Pr[\mathsf{Win}_2]| \leqslant \Pr[\mathsf{Coll}].$$

We bound $\Pr[\mathsf{Coll}]$ via the following reduction. On input h, $\mathcal{B}_3$ simulates Game_3 honestly except that we publish h in mpk and $\mathsf{pk}^*_{\mathsf{ots}}$ is created before $\mathcal{B}_3$ answers any queries. This will not change the view of $\mathcal{A}$ since $\mathsf{pk}^*_{\mathsf{ots}}$ is independent of (m_0, m_1, S_0, S_1). Once Coll happens when answering query with $(\mathsf{ct}_1, \mathsf{pk}_{\mathsf{ots}}, \sigma)$, $\mathcal{B}_3$ outputs $(\mathsf{pk}_{\mathsf{ots}}, \mathsf{pk}^*_{\mathsf{ots}})$ as a collision. This readily proves the lemma. □

Proof of Lemma 5: We prove the lemma via the following hybrid argument:

$$\mathsf{Game}_3 = \mathsf{Game}_{3.0} \approx_s \mathsf{Game}_{3.1} \approx_s \mathsf{Game}_{3.2} \approx_s \cdots \approx_s \mathsf{Game}_{3.q_D} = \mathsf{Game}_4$$

where $\mathsf{Game}_{3.j}$, for all $j \in [0, q_D]$, is the same as Game_3 except that for the first j queries sent to DecO, we introduce condition $(\mathfrak{d})$.

Let $\mathsf{BadSpan}_j$ be the event that the j-th query is rejected in $\mathsf{Game}_{3.j}$ but is replied with $m' \neq \perp$ in $\mathsf{Game}_{3.j-1}$. We prove the theorem by showing that

$$|\Pr[\mathsf{Win}_{3.j-1}] - \Pr[\mathsf{Win}_{3.j}]| \leqslant \Pr[\mathsf{BadSpan}_j] \quad \text{for all } j \in [q_D].$$

Let $(\mathsf{ct} = ([\mathbf{u}^\top], c_1, \nu_1, \ldots, c_\ell, \nu_\ell, \mathsf{pk}_{\mathsf{ots}}, \sigma), i)$ be the j-th query. The event $\mathsf{BadSpan}_j$ can be restated as follows: the j-th query survives under condition $(a), (b), (c')$ with $\mathbf{u} \notin \mathsf{span}(\mathbf{A})$ but there exists $i' \in [\ell]$ such that $\nu_{i'} = [\mathbf{u}^\top(\mathbf{x}_i + \alpha \cdot \mathbf{y}_i)]$. To bound $\Pr[\mathsf{BadSpan}_j]$, we introduce another event $\mathsf{BadSpan}'_j$ which is defined exactly as $\mathsf{BadSpan}_j$ except that we replace $[\mathbf{u}^\top(\mathbf{x}_i + \alpha \cdot \mathbf{y}_i)]$ with a random group element $[\nu] \leftarrow_R \mathbb{G}$. Firstly, since ν is independent of $\mathcal{A}$'s behaviour, we have that

$$\Pr[\mathsf{BadSpan}'_j] = \ell/p.$$

Secondly, we claim that

$$\Pr[\mathsf{BadSpan}_j] = \Pr[\mathsf{BadSpan}'_j].$$

This follows from the fact that, for all $Q_{\mathsf{sk}} \in [n]$, all $S_b \in [n]$ and all $i \in [n] \setminus Q_{\mathsf{sk}}$, we have

$$\begin{pmatrix} \mathsf{mpk}, \mathsf{DecO}: & \mathbf{A}, \{\mathbf{A}^\top \mathbf{x}_\eta, \mathbf{A}^\top \mathbf{y}_\eta\}_{\eta \in [n]} \\ \mathsf{KeyO}: & \{\mathbf{x}_\eta, \mathbf{y}_\eta\}_{\eta \in Q_{\mathsf{sk}}} \\ \mathsf{ct}^*: & \{\mathbf{u}^{*\top}(\mathbf{x}_\eta + \alpha^* \cdot \mathbf{y}_\eta)\}_{\eta \in S_b} \\ \to \mathsf{DecO}: & \mathbf{u}^\top(\mathbf{x}_i + \alpha \cdot \mathbf{y}_i) \end{pmatrix} \equiv \begin{pmatrix} \mathbf{A}, \{\mathbf{A}^\top \mathbf{x}_\eta, \mathbf{A}^\top \mathbf{y}_\eta\}_{\eta \in [n]} \\ \{\mathbf{x}_\eta, \mathbf{y}_\eta\}_{\eta \in Q_{\mathsf{sk}}} \\ \{\mathbf{u}^{*\top}(\mathbf{x}_\eta + \alpha^* \cdot \mathbf{y}_\eta)\}_{\eta \in S_b} \\ \nu \end{pmatrix}$$

when $\mathbf{x}_\eta, \mathbf{y}_\eta \leftarrow_R \mathbb{Z}_p^{k+1}$ for all $\eta \in [n]$ and $\nu \leftarrow_R \mathbb{Z}_p$ for all $\mathbf{u}, \mathbf{u}^* \notin \mathsf{span}(\mathbf{A})$. We note that (1) the first $j-1$ decryption queries leak no more information than mpk since all queries with $\mathbf{u} \notin \mathsf{span}(\mathbf{A})$ will be rejected (see the first line); (2) we naturally assume that $i \notin Q_{\mathsf{sk}}$, otherwise the adversary can simulate DecO (on this query) by itself; (3) two distributions are *perfectly* identical, so our non-adaptive statement implies the adaptive one. This readily proves the lemma. □

Proof of Lemma 6: We will prove that $\Pr[\mathsf{Win}_4] = 1/2$ in two cases. Combining them together immediately proves the lemma.

Case 1: $Q_{\mathsf{sk}} \cap (S_0 \cap S_1) = \emptyset$. We claim that (c_j^*, ν_j^*) are uniformly distributed over $\mathbb{G}^2$ for all $j \in [\ell]$. This means that ct^* is actually independent of b and the adversary's advantage is 0 in this case. This follows from the fact that, for all $Q_{\mathsf{sk}} \subseteq [n]$ and all $S_b \subseteq [n]$ satisfying $Q_{\mathsf{sk}} \cap S_b = \emptyset$, we have

$$\begin{pmatrix} \mathsf{mpk}, \mathsf{DecO}: & \mathbf{A}, \{\mathbf{A}^\top \mathbf{k}_\eta, \mathbf{A}^\top \mathbf{x}_\eta, \mathbf{A}^\top \mathbf{y}_\eta\}_{\eta \in [n]} \\ \mathsf{KeyO}: & \{\mathbf{k}_\eta, \mathbf{x}_\eta, \mathbf{y}_\eta\}_{\eta \in Q_{\mathsf{sk}}} \\ \to \mathsf{ct}^*: & \{\mathbf{u}^{*\top}\mathbf{k}_\eta, \mathbf{u}^{*\top}(\mathbf{x}_\eta + \alpha^* \cdot \mathbf{y}_\eta)\}_{\eta \in S_b} \end{pmatrix} \equiv \begin{pmatrix} \mathbf{A}, \{\mathbf{A}^\top \mathbf{k}_\eta, \mathbf{A}^\top \mathbf{x}_\eta, \mathbf{A}^\top \mathbf{y}_\eta\}_{\eta \in [n]} \\ \{\mathbf{k}_\eta, \mathbf{x}_\eta, \mathbf{y}_\eta\}_{\eta \in Q_{\mathsf{sk}}} \\ \{\tilde{c}_\eta^*, \tilde{\nu}_\eta^*\}_{\eta \in S_b} \end{pmatrix}$$

when $\mathbf{k}_\eta, \mathbf{x}_\eta, \mathbf{y}_\eta \leftarrow_R \mathbb{Z}_p^{k+1}$ for all $\eta \in [n]$ and $\tilde{c}_\eta^*, \tilde{\nu}_\eta^* \leftarrow_R \mathbb{Z}_p$ for all $\eta \in S_b$ if $\mathbf{u}^* \notin \mathsf{span}(\mathbf{A})$.

Case 2: $Q_{\mathsf{sk}} \cap (S_0 \cap S_1) \neq \emptyset$. We claim that all (c_j^*, ν_j^*) such that $i_{\tau(j),b} \in S_b \setminus S_{1-b}$ are uniformly distributed over $\mathbb{G}^2$. This follows from a statistical statement identical to that in Case 1 except that (c_j^*, ν_j^*) with $i_{\tau(j),b} \in S_b \cap S_{1-b}$ remain unchanged. The claim is sufficient to argue that ct^* reveals nothing about b since it must hold that $m_0 = m_1$ in this case. □

4 Tightly Secure ANOBE with Shorter Ciphertext

4.1 Construction

– $\mathsf{Setup}\ (1^\lambda, n)$: Run $\mathcal{PG} := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2) \leftarrow_R \mathsf{PGGen}(1^\lambda)$. Sample

$$\mathbf{A}, \mathbf{B} \leftarrow_R \mathcal{D}_k,\ \mathbf{X}, \mathbf{Y} \leftarrow_R \mathbb{Z}_p^{(k+1)\times(k+1)},\ \mathbf{k}_i \leftarrow_R \mathbb{Z}_p^{k+1}\ \text{ for } i \in [n].$$

Select a key-binding secure symmetric encryption scheme (E, D) with the key space $\mathcal{K} := \mathbb{G}_1$ and a collision-resilient hash function $h \leftarrow_R \mathcal{H}$ mapping from $\{0,1\}^*$ to $\mathbb{Z}_p$. The master public key is

$$\mathsf{mpk} := \left(\mathcal{PG}, (\mathsf{E}, \mathsf{D}), h; \begin{array}{ll} [\mathbf{A}^\top]_1, \{[\mathbf{A}^\top \mathbf{k}_i]_1\}_{i=1}^n, [\mathbf{A}^\top \mathbf{X}]_1, [\mathbf{A}^\top \mathbf{Y}]_1 \\ [\mathbf{B}]_2, \qquad\qquad\qquad [\mathbf{X}\mathbf{B}]_2, \quad [\mathbf{Y}\mathbf{B}]_2 \end{array} \right)$$

and the master secret key is $\mathsf{msk} := \{\mathbf{k}_i\}_{i=1}^n$.

– $\mathsf{KeyGen}\ (\mathsf{msk}, \mathsf{mpk}, i)$: Output the secret key $\mathsf{sk}_i := \mathbf{k}_i$.

– $\mathsf{Enc}\ (\mathsf{mpk}, m, S)$: Let $\ell := |S|$ and $S = \{i_1, \ldots, i_\ell\} \subseteq \mathcal{U}$. Sample $\mathbf{r} \leftarrow_R \mathbb{Z}_p^k$ and compute

$$[\mathbf{u}^\top]_1 := [\mathbf{r}^\top \mathbf{A}^\top]_1.$$

Select session key $K \leftarrow_R \mathbb{G}_1$ and compute

$$c_0 := \mathsf{E}_K(m),\ c_1 := [\mathbf{r}^\top \mathbf{A}^\top \mathbf{k}_{i_1}]_1 \cdot K,\ \ldots,\ c_\ell := [\mathbf{r}^\top \mathbf{A}^\top \mathbf{k}_{i_\ell}]_1 \cdot K$$

Choose a random permutation τ over $[\ell]$ and compute

$$[\boldsymbol{\pi}]_1 := [\mathbf{r}^\top \mathbf{A}^\top (\mathbf{X} + \alpha \cdot \mathbf{Y})]_1$$

where $\alpha := h([\mathbf{u}^\top]_1, c_0, c_{\tau(1)}, \ldots, c_{\tau(\ell)})$. The ciphertext is

$$\mathsf{ct} := (\ [\mathbf{u}^\top]_1,\ c_0,\ c_{\tau(1)},\ \ldots,\ c_{\tau(\ell)},,\ [\boldsymbol{\pi}]_1\ ).$$

– $\mathsf{Dec}(\mathsf{mpk}, \mathsf{ct}, \mathsf{sk}_i)$: Parse ct as $([\mathbf{u}^\top]_1, c_0, \bar{c}_1, \ldots, \bar{c}_\ell, [\boldsymbol{\pi}]_1)$ and sk_i as $\mathbf{k}_i$. Compute

$$\alpha = h([\mathbf{u}^\top]_1, c_0, \bar{c}_1, \ldots, \bar{c}_\ell)$$

and check

$$e([\boldsymbol{\pi}]_1, [\mathbf{B}]_2) \stackrel{?}{=} e([\mathbf{u}^\top]_1, [(\mathbf{X} + \alpha \cdot \mathbf{Y})\mathbf{B}]_2). \tag{1}$$

If Equation (1) does not hold, return $\perp$; otherwise, do the following two steps from $j := 1$.

1. Compute $K' := \bar{c}_j / [\mathbf{u}^\top \mathbf{k}_i]_1$ and $m' := \mathsf{D}_{K'}(c_0)$. If $m' \neq \perp$, return m' and halt; otherwise, go to the second step.
2. If $j = \ell$, return $\perp$ and halt; otherwise, do the first step with $j := j + 1$.

Correctness. For any ciphertext $\mathsf{ct} := ([\mathbf{u}^\top]_1, c_0, \bar{c}_1, \ldots, \bar{c}_\ell, [\boldsymbol{\pi}]_1)$ for set $S \subseteq U$ produced by Enc, we have

$$e([\boldsymbol{\pi}]_1, [\mathbf{B}]_2) = e([\mathbf{r}^\top \mathbf{A}^\top (\mathbf{X} + \alpha \cdot \mathbf{Y})]_1, [\mathbf{B}]_2) = e([\mathbf{u}^\top]_1, [(\mathbf{X} + \alpha \cdot \mathbf{Y})\mathbf{B}]_2)$$

where $\alpha = \mathsf{h}([\mathbf{u}^\top]_1, c_0, \bar{c}_1, \ldots, \bar{c}_\ell)$. That is the ciphertext always satisfies Equation (1). Given a secret key $\mathsf{sk}_i = \mathbf{k}_i$ for $i \in S$, we know that there exists $i' \in [\ell]$ such that $c_{i'} = [\mathbf{r}^\top \mathbf{A}^\top \mathbf{k}_i]_1 \cdot K$. The correctness of our ANOBE then follows from the following two observations:

1. For each $j < i'$, we know that $c_j = [\mathbf{r}^\top \mathbf{A}^\top \mathbf{k}_{j'}]_1 \cdot K$ for some $j' \in S \setminus \{i\}$, and thus we have

   $$c_j / [\mathbf{u}^\top \mathbf{k}_i]_1 \neq K$$

   with overwhelming probability. From the key-binding feature of (E, D), the decryption algorithm Dec will return nothing before the i'-th iteration.
2. It is easy to see that

   $$c_{i'} / [\mathbf{u}^\top \mathbf{k}_i]_1 = K.$$

   By the correctness of (E, D), the decryption algorithm Dec will return m in the i'-th iteration.

4.2 Security Result and Proof Overview

We prove the following theorem.

Theorem 2 *Our broadcast encryption described in Section 4.1 is ANO-IND-CCA secure assuming that: (1) $\mathcal{H}$ is collision-resistant; (2) the $\mathcal{D}_k$-MDDH assumption holds in $\mathbb{G}_1$; (3) the $\mathcal{D}_k$-KerMDH assumptions holds in $\mathbb{G}_2$; (4) (E, D) is semantically secure. Concretely, for any adversary $\mathcal{A}$, there exist algorithms $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3, \mathcal{B}_4$, such that*

$$\mathsf{Adv}^{\mathsf{BE}}_{\mathcal{A}}(\lambda) \leqslant \mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{B}_1, \mathbb{G}_1}(\lambda) + \mathsf{Adv}^{\mathsf{hash}}_{\mathcal{B}_2}(\lambda) + \mathsf{Adv}^{\mathsf{kmdh}}_{\mathcal{B}_3, \mathbb{G}_2}(\lambda) + 2 \cdot \mathsf{Adv}^{\mathsf{se}}_{\mathcal{B}_4}(\lambda) + O(1/p)$$

and $\mathsf{Time}(\mathcal{B}_1), \mathsf{Time}(\mathcal{B}_2), \mathsf{Time}(\mathcal{B}_3), \mathsf{Time}(\mathcal{B}_4) \approx \mathsf{Time}(\mathcal{A})$.

We prove the theorem via the following game sequence.

Game_0**.** This game is identical to the real game described in Section 2.1. In particular, our simulation is as follows:

Setup. Run $\mathsf{Setup}(1^\lambda, n)$ and send $\mathcal{A}$ the master public key

$$\mathsf{mpk} := \left(\mathcal{PG}, (\mathsf{E}, \mathsf{D}), \mathsf{h}; \begin{array}{lll} [\mathbf{A}^\top]_1, \{[\mathbf{A}^\top \mathbf{k}_i]_1\}_{i=1}^n, [\mathbf{A}^\top \mathbf{X}]_1, [\mathbf{A}^\top \mathbf{Y}]_1 \\ [\mathbf{B}]_2, \qquad\qquad [\mathbf{X}\mathbf{B}]_2, \quad [\mathbf{Y}\mathbf{B}]_2 \end{array} \right)$$

and keep the master secret key $\mathsf{msk} := \{\mathbf{k}_i\}_{i=1}^n$ as well as $\mathbf{X}, \mathbf{Y}$. We also set $Q_{\mathsf{sk}} := \emptyset$.

Challenge ciphertext. Receiving (m_0, m_1, S_0, S_1) from $\mathcal{A}$ where we let $S_0 = \{i_{1,0}, \ldots, i_{\ell,0}\}$ and $S_1 = \{i_{1,1}, \ldots, i_{\ell,1}\}$, pick $b \leftarrow_R \{0,1\}$, $\mathbf{u}^* \leftarrow_R \mathsf{span}(\mathbf{A})$, $K^* \leftarrow_R \mathbb{G}_1$ and choose a random permutation τ, and compute

$$\mathsf{ct}_1^* := ([\mathbf{u}^{*\top}]_1, c_0^*, c_1^*, \ldots, c_\ell^*)$$

where $c_j^* = [\mathbf{u}^{*\top}\mathbf{k}_{i_{\tau(j),b}}]_1 \cdot K^*$ for all $j \in [\ell]$ and $c_0^* = \mathsf{E}_{K^*}(m_b)$. Compute $\alpha^* = \mathsf{H}(\mathsf{ct}_1^*)$ and output the challenge ciphertext

$$\mathsf{ct}^* := (\ \mathsf{ct}_1^*,\ [\boldsymbol{\pi}^*]_1 := [\mathbf{u}^{*\top}(\mathbf{X} + \alpha^* \cdot \mathbf{Y})]_1\ ).$$

Simulating KeyO**.** On input $i \in U$, output $\mathbf{k}_i$ and update $Q_{\mathsf{sk}} := Q_{\mathsf{sk}} \cup \{i\}$.
Simulating DecO**.** On input (ct, i), parse

$$\mathsf{ct} = (\mathsf{ct}_1 = ([\mathbf{u}^\top]_1, c_1, \ldots, c_\ell, c_0), [\boldsymbol{\pi}]_1),$$

compute $\alpha = \mathsf{h}(\mathsf{ct}_1)$ and reject the query (by returning $\perp$) if

$$(a) \quad \mathsf{ct} = \mathsf{ct}^*$$

$$\text{or} \quad (b) \quad e([\boldsymbol{\pi}]_1, [\mathbf{B}]_2) \neq e([\mathbf{u}^\top]_1, [(\mathbf{X} + \alpha \cdot \mathbf{Y})\mathbf{B}]_2).$$

Then recover m using $\mathbf{k}_i$ as Dec and return m.
Finalize. Received b' from $\mathcal{A}$, return 1 if $b = b'$; otherwise return 0.

We let Win_i denote the event that $\mathcal{A}$ guesses b correctly in Game_i. Since Game_0 perfectly simulates the real game, we have $\mathsf{Adv}^{\mathsf{BE}}_{\mathcal{A}}(1^\lambda) = |\Pr[\mathsf{Win}_0] - 1/2|$.

Game_1**.** This game is identical to Game_0 except that we sample $\mathbf{u}^* \leftarrow_R \mathbb{Z}_p^{k+1}$ when generating the challenge ciphertext ct^*. This game is indistinguishable from Game_0 under the $\mathcal{D}_k$-MDDH assumption. Formally, we have the following lemma and the proof is analgous to that for Lemma 2.

Lemma 7 ($\mathsf{Game}_1 \approx_c \mathsf{Game}_0$)**.** *There exists an adversary $\mathcal{B}_1$ such that*

$$|\Pr[\mathsf{Win}_1] - \Pr[\mathsf{Win}_0]| \leqslant \mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{B}_1,\mathbb{G}_1}(\lambda)$$

Game_2**.** This game is identical to Game_1 except that DecO, on input (ct, i), returns $\perp$ if (a) or (b) or

$$(c) \quad \mathsf{ct}_1 \neq \mathsf{ct}_1^* \text{ but } \alpha = \alpha^*.$$

By the collision-resilience of $\mathcal{H}$, this game is indistinguishable from Game_1. Formally, we have the following lemma and the proof is similar to that for Lemma 4.

Lemma 8 ($\mathsf{Game}_2 \approx_c \mathsf{Game}_1$)**.** *There exists an algorithm $\mathcal{B}_2$ such that*

$$|\Pr[\mathsf{Win}_2] - \Pr[\mathsf{Win}_1]| \leqslant \mathsf{Adv}^{\mathsf{hash}}_{\mathcal{B}_2}(\lambda)$$

Game_3**.** This game is identical to Game_2 except the following substitution:

$$(b)\ e([\boldsymbol{\pi}]_1, [\mathbf{B}]_2) \neq e([\mathbf{u}^\top]_1, [(\mathbf{X} + \alpha \cdot \mathbf{Y})\mathbf{B}]_2) \longmapsto (b')\ [\boldsymbol{\pi}]_1 \neq [\mathbf{u}^\top(\mathbf{X} + \alpha \cdot \mathbf{Y})]_1.$$

This game is the same as Game_2 until $\mathcal{A}$ sends DecO a query which is rejected by condition (b') but survives under condition (b). One can see that such a query immediately gives a solution to the $\mathcal{D}_k$-KerMDH problem w.r.t $[\mathbf{B}]_2$. Formally, we have the following lemma.

Lemma 9 ($\mathsf{Game}_3 \approx_c \mathsf{Game}_2$). *There exists an algorithm $\mathcal{B}_3$ such that*

$$|\Pr[\mathsf{Win}_3] - \Pr[\mathsf{Win}_2]| \leqslant \mathsf{Adv}^{\mathsf{kmdh}}_{\mathcal{B}_3,\mathbb{G}_2}(\lambda)$$

Game_4. This game is identical to Game_3 except the following substitution

$$(b')\ [\boldsymbol{\pi}]_1 \neq [\mathbf{u}^\top(\mathbf{X}+\alpha\cdot\mathbf{Y})]_1 \longmapsto (b'')\ \mathbf{u} \notin \mathsf{span}(\mathbf{A}) \parallel [\boldsymbol{\pi}]_1 \neq [\mathbf{u}^\top(\mathbf{X}+\alpha\cdot\mathbf{Y})]_1.$$

Here "$\parallel$" denotes the OR operation which neglects the second operand if the first one is satisfied. We have the following lemma stating that this game is statistically close to Game_3.

Lemma 10 ($\mathsf{Game}_4 \approx_s \mathsf{Game}_3$). $|\Pr[\mathsf{Win}_4] - \Pr[\mathsf{Win}_3]| \leqslant O(1/p)$.

Let q_D be the number of decryption queries. The lemma will be proved in q_D steps. In the j-th step, assuming that the first $j-1$ decryption queries have been processed with condition (b''), we demonstrate that the j-th query with $\mathbf{u} \notin \mathsf{span}(\mathbf{A})$ can be rejected by condition $(a), (b'), (c)$ with high probability. This simply follows from Lemma 1 (the core lemma).

To complete the proof of Theorem 2, we show the following lemma.

Lemma 11 (**Bounding** $\Pr[\mathsf{Win}_4]$). *There exists an algorithm $\mathcal{B}_4$ such that*

$$\Pr[\mathsf{Win}_4] \leqslant 1/2 + 2\cdot\mathsf{Adv}^{\mathsf{se}}_{\mathcal{B}_4}(\lambda)$$

To prove the lemma, we consider two cases: (1) when $Q_{sk} \cap (S_0 \cap S_1) = \emptyset$, we can prove that $[\mathbf{u}^{*\top}\mathbf{k}_i]_1$ for $i \in S_b$ are independently and uniformly distributed over $\mathbb{G}_1$, which hide both S_b and K^*. The proof is similar to the proof of Lemma 6. Then the semantic security of (E, D) allows us to hide m_b; (2) when $Q_{sk} \cap (S_0 \cap S_1) \neq \emptyset$, we can only prove that $[\mathbf{u}^{*\top}\mathbf{k}_i]_1$ for $i \in S_b \setminus S_{1-b}$ are randomly distributed, but it is sufficient for proving the lemma since $m_0 = m_1$.

4.3 Two Simple Missing Proofs

Proof of Lemma 9: In Game_3, define BadKer the event that $\mathcal{A}$ sends DecO a query which is rejected by condition (b'), but survives under condition (b). It is easy to see that if BadKer does not occur, Game_3 is identical to Game_2. Namely we have

$$|\Pr[\mathsf{Win}_3] - \Pr[\mathsf{Win}_2]| \leqslant \Pr[\mathsf{BadKer}].$$

We bound $\Pr[\mathsf{BadKer}]$ via the following reduction. On input $[\mathbf{B}]_2$, $\mathcal{B}_3$ samples $\mathbf{X}, \mathbf{Y} \leftarrow_R \mathbb{Z}_p^{(k+1)\times(k+1)}$ and simulates Game_3 honestly using $[\mathbf{B}]_2$. Once BadKer happens when answering query with $\mathsf{ct} = (\mathsf{ct}_1 = ([\mathbf{u}^\top]_1, c_0, c_1, \ldots, c_\ell), [\boldsymbol{\pi}]_1)$, $\mathcal{B}_3$ computes and outputs

$$[\mathbf{t}^\top := \boldsymbol{\pi} - \mathbf{u}^\top(\mathbf{X} + h(\mathsf{ct}_1)\cdot\mathbf{Y})]_1.$$

We note that (1) the query has been rejected by condition (b'), we have $\mathbf{t} \neq \mathbf{0}$; (2) the condition (b) ensures that $\mathbf{t} \in \mathsf{Ker}(\mathbf{B})$. This readily proves the lemma. □

Proof of Lemma 10: We prove the lemma via the following hybrid argument:

$$\mathsf{Game}_3 = \mathsf{Game}_{3.0} \approx_s \mathsf{Game}_{3.1} \approx_s \mathsf{Game}_{3.2} \approx_s \cdots \approx_s \mathsf{Game}_{3.q_D} = \mathsf{Game}_4$$

where $\mathsf{Game}_{3.j}$, for all $j \in [0, q_D]$, is the same as Game_3 except that for the first j queries sent to DecO, the condition (b') is replaced by condition (b'').

Let $\mathsf{BadSpan}_j$ be the event that the j-th query is rejected in $\mathsf{Game}_{3.j}$ but survives in $\mathsf{Game}_{3.j-1}$. We have that

$$|\Pr[\mathsf{Win}_{3,j-1}] - \Pr[\mathsf{Win}_{3,j}]| \leqslant \Pr[\mathsf{BadSpan}_j].$$

The event $\mathsf{BadSpan}_j$ can be restated as follows: the j-th query survives under condition $(a), (b'), (c)$ with $\mathbf{u} \notin \mathsf{span}(\mathbf{A})$. We first claim that $\alpha \neq \alpha^*$. Then Lemma 1, the core lemma, immediately implies that $\Pr[\mathsf{BadSpan}_j] < 1/p$. The observation is we leak no more information than $\mathbf{A}^\top\mathbf{X}, \mathbf{A}^\top\mathbf{Y}$ when answering the first $j-1$ queries to DecO due to the newly introduced condition $\mathbf{u} \notin \mathsf{span}(\mathbf{A})$.

Let the j-th query be associated with $(\mathsf{ct}_1, \boldsymbol{\pi})$. We justify the claim $(\alpha \neq \alpha^*)$ as follows. Thanks to condition (c), we only need to show that $\mathsf{ct}_1 \neq \mathsf{ct}_1^*$. We suppose $\mathsf{ct}_1 = \mathsf{ct}_1^*$. Observe that, (1) when $\boldsymbol{\pi} \neq \boldsymbol{\pi}^*$, the query will be rejected by condition (b'); (2) when $\boldsymbol{\pi} = \boldsymbol{\pi}^*$, the query will be rejected by condition (a). This readily proves the claim and thus complete the proof of the lemma. □

4.4 Proof for Lemma 11

We will prove Lemma 11 by considering two cases. Let Win_4^1 and Win_4^2 denote that event Win_4 occurs in Case 1 and Case 2, respectively. This notation also applies to all later events.

Case 1: $\mathbf{Q}_{\mathsf{sk}} \cap (\mathbf{S_0} \cap \mathbf{S_1}) = \emptyset$. We define the following two auxiliary games.

Game_5. This game is identical to Game_4 except that we pick

$$c_j^* \leftarrow_R G_1 \text{ for all } j \in [\ell].$$

This game is statistically indistinguishable with Game_4, which follows that fact that all $[\mathbf{u}^{*\top}\mathbf{k}_i]_1$ in ct_1^* is independently and uniformly distributed conditioned on mpk, KeyO and DecO. Formally, we show the following lemma. The proof is quite similar to the proof for Lemma 6 (Case 1).

Lemma 12 ($\mathsf{Game}_4 \approx_s \mathsf{Game}_5$). $\Pr[\mathsf{Win}_4^1] = \Pr[\mathsf{Win}_5^1]$.

Game_6. This game is identical to Game_5 except that we compute

$$c_0 \leftarrow_R \mathsf{E}_{K^*}(0)$$

This game is indistinguishable with Game_5 due to the semantic security of (E, D). Formally, we have the following lemma.

Lemma 13 ($\mathsf{Game}_6 \approx_c \mathsf{Game}_5$). *There exists an algorithm $\mathcal{B}_4$ such that*

$$|\Pr[\mathsf{Win}_6^1] - \Pr[\mathsf{Win}_5^1]| \leqslant 2 \cdot \mathsf{Adv}^{\mathsf{se}}_{\mathcal{B}_4}(\lambda)$$

and $\mathsf{Time}(\mathcal{B}_4) \approx \mathsf{Time}(\mathcal{A})$.

Observe that the challenge ciphertext ct^* in Game_6 is independent of b and we have that $\Pr[\mathsf{Win}_6^1] = 1/2$. This immediately gives the following bound.

$$\Pr[\mathsf{Win}_4^1] \leqslant 1/2 + 2 \cdot \mathsf{Adv}^{\mathsf{se}}_{\mathcal{B}_4}(\lambda).$$

We now provide the full proof of Lemma 13 which completes our proof.

Proof of Lemma 13: We construct $\mathcal{B}_4$ as follows. On input (E, D), $\mathcal{B}_4$ prepares mpk honestly as in Game_5 using the input. Both KeyO and DecO can be simulated honestly.

For the challenge ciphertext, $\mathcal{B}_4$ samples $[\mathbf{u}^*]_1$ and $c_1^*, \ldots, c_\ell^*$ as in Game_5. Then it picks $b \leftarrow_R \{0,1\}$ and submits $(m_b, 0)$ to the environment, the ciphertext returned is set to be c_0^*. Finally, the last component $[\boldsymbol{\pi}^*]_1$ is computed as in Game_5.

Observe that, when $c_0^* \leftarrow_R \mathsf{E}_{K^*}(m_b)$ for some random K^*, our simulation is identical to Game_5; otherwise, when $c_0^* \leftarrow_R \mathsf{E}_{K^*}(0)$, our simulation is identical to Game_6. This readily proves the lemma. □

Case 2: $\mathbf{Q}_{\mathsf{sk}} \cap (\mathbf{S_0} \cap \mathbf{S_1}) \neq \emptyset$. We define the following auxiliary game.

Game_5**.** This game is identical to Game_4 except that we pick

$$c_i^* \leftarrow_R \mathbb{G}_1 \quad \text{for all } i \in S_b \setminus S_{1-b}.$$

This game is statistically indistinguishable from Game_4, which follows from the fact that all $\mathbf{u}^{*\top}\mathbf{k}_i$ with $i \in S_b \setminus S_{1-b}$ are uniformly distributed over $\mathbb{Z}_p$ conditioned on mpk, KeyO and DecO. Formally, we show the following lemma. The proof is quite similar to the proof for Lemma 6 (Case 2).

Lemma 14 ($\mathsf{Game}_5 \approx_s \mathsf{Game}_4$ **in Case 2).** $\Pr[\mathsf{Win}_5^2] = \Pr[\mathsf{Win}_4^2]$.

Observe that we only need to know $S_0 \cap S_1$ in order to generate $c_1^*, \ldots, c_\ell^*$ in Game_5 and they do not leak b. Furthermore c_0^* does not leak b since $m_0 = m_1$ in Case 2. Therefore we have $\Pr[\mathsf{Win}_5^2] = 1/2$ and thus

$$\Pr[\mathsf{Win}_4^2] \leqslant 1/2.$$

Final Analysis. Let Case1 and Case2 be the events that $\mathcal{A}$ outputs (S_0, S_1) in Case 1 and Case 2, respectively. Because $\Pr[\mathsf{Case1}] + \Pr[\mathsf{Case2}] = 1$, we have

$$\begin{aligned}
\Pr[\mathsf{Win}_4] &= \Pr[\mathsf{Win}_4^1] \cdot \Pr[\mathsf{Case1}] + \Pr[\mathsf{Win}_4^2] \cdot \Pr[\mathsf{Case2}] \\
&\leqslant 1/2 + 2 \cdot \mathsf{Adv}^{\mathsf{se}}_{\mathcal{B}_4}(\lambda) \cdot \Pr[\mathsf{Case1}] \\
&\leqslant 1/2 + 2 \cdot \mathsf{Adv}^{\mathsf{se}}_{\mathcal{B}_4}(\lambda).
\end{aligned}$$

This completes the proof of Lemma 11.

5 Conclusion

In this paper, we described two concrete ANOBE schemes. The first one is an instantiation of Libert *et al.*'s generic ANOBE. However, by working out the proof directly, we achieved a constantly tight reduction to standard assumptions. Furthermore, we pointed out that this scheme supports fast decryption for free and thus enjoys shorter ciphertexts. By the second scheme, we showed how to shorten the ciphertext again while preserving the tightness at the cost of slower decryption.

Acknowledgment. We greatly thank Benoît Libert for his encouragement and support. We also thank all anonymous reviewers for their constructive comments.

References

ABN10. Michel Abdalla, Mihir Bellare, and Gregory Neven. Robust encryption. In Daniele Micciancio, editor, *TCC 2010*, volume 5978 of *LNCS*, pages 480–497. Springer, Heidelberg, February 2010. 4, 15

BBS03. Mihir Bellare, Alexandra Boldyreva, and Jessica Staddon. Randomness re-use in multi-recipient encryption schemeas. In Yvo Desmedt, editor, *PKC 2003*, volume 2567 of *LNCS*, pages 85–99. Springer, Heidelberg, January 2003. 4

BBW06. Adam Barth, Dan Boneh, and Brent Waters. Privacy in encrypted content distribution using private broadcast encryption. In Giovanni Di Crescenzo and Avi Rubin, editors, *FC 2006*, volume 4107 of *LNCS*, pages 52–64. Springer, Heidelberg, February / March 2006. 3, 4

Ber91. Shimshon Berkovits. How to broadcast a secret (rump session). In Donald W. Davies, editor, *EUROCRYPT'91*, volume 547 of *LNCS*, pages 535–541. Springer, Heidelberg, April 1991. 3

BGW05. Dan Boneh, Craig Gentry, and Brent Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In Victor Shoup, editor, *CRYPTO 2005*, volume 3621 of *LNCS*, pages 258–275. Springer, Heidelberg, August 2005. 3

BSW11. Dan Boneh, Amit Sahai, and Brent Waters. Functional encryption: Definitions and challenges. In Yuval Ishai, editor, *TCC 2011*, volume 6597 of *LNCS*, pages 253–273. Springer, Heidelberg, March 2011. 3

CCS09. Jan Camenisch, Nishanth Chandran, and Victor Shoup. A public key encryption scheme secure against key dependent chosen plaintext and adaptive chosen ciphertext attacks. In Antoine Joux, editor, *EUROCRYPT 2009*, volume 5479 of *LNCS*, pages 351–368. Springer, Heidelberg, April 2009. 5

CGW15. Jie Chen, Romain Gay, and Hoeteck Wee. Improved dual system ABE in prime-order groups via predicate encodings. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 595–624. Springer, Heidelberg, April 2015. 3

CHK04. Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-ciphertext security from identity-based encryption. In Christian Cachin and Jan Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 207–222. Springer, Heidelberg, May 2004. 4

CS98. Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In Hugo Krawczyk, editor, *CRYPTO'98*, volume 1462 of *LNCS*, pages 13–25. Springer, Heidelberg, August 1998. 4, 5, 6, 7

CS02. Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In Lars R. Knudsen, editor, *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 45–64. Springer, Heidelberg, April / May 2002. 4, 5, 6, 7

DPP07. Cécile Delerablée, Pascal Paillier, and David Pointcheval. Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys. In Tsuyoshi Takagi, Tatsuaki Okamoto, Eiji Okamoto, and Takeshi Okamoto, editors, *PAIRING 2007*, volume 4575 of *LNCS*, pages 39–59. Springer, Heidelberg, July 2007. 3

EHK+13. Alex Escala, Gottfried Herold, Eike Kiltz, Carla Ràfols, and Jorge Villar. An algebraic framework for Diffie-Hellman assumptions. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 129–147. Springer, Heidelberg, August 2013. 9

Fis99. Marc Fischlin. Pseudorandom function tribe ensembles based on one-way permutations: Improvements and applications. In Jacques Stern, editor, *EUROCRYPT'99*, volume 1592 of *LNCS*, pages 432–445. Springer, Heidelberg, May 1999. 10

FN94. Amos Fiat and Moni Naor. Broadcast encryption. In Douglas R. Stinson, editor, *CRYPTO'93*, volume 773 of *LNCS*, pages 480–491. Springer, Heidelberg, August 1994. 3

FP12. Nelly Fazio and Irippuge Milinda Perera. Outsider-anonymous broadcast encryption with sublinear ciphertexts. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *PKC 2012*, volume 7293 of *LNCS*, pages 225–242. Springer, Heidelberg, May 2012. 4

GHKW16. Romain Gay, Dennis Hofheinz, Eike Kiltz, and Hoeteck Wee. Tightly CCA-secure encryption without pairings. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part I*, volume 9665 of *LNCS*, pages 1–27. Springer, Heidelberg, May 2016. 6

GPSW06. Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors, *ACM CCS 06*, pages 89–98. ACM Press, October / November 2006. Available as Cryptology ePrint Archive Report 2006/309. 3

Gro06. Jens Groth. Simulation-sound NIZK proofs for a practical language and constant size group signatures. In Xuejia Lai and Kefei Chen, editors, *ASIACRYPT 2006*, volume 4284 of *LNCS*, pages 444–459. Springer, Heidelberg, December 2006. 5

GW09. Craig Gentry and Brent Waters. Adaptive security in broadcast encryption systems (with short ciphertexts). In Antoine Joux, editor, *EUROCRYPT 2009*, volume 5479 of *LNCS*, pages 171–188. Springer, Heidelberg, April 2009. 3

Hof17. Dennis Hofheinz. Adaptive partitioning. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part II*, volume 10211 of *LNCS*, pages 489–518. Springer, Heidelberg, May 2017. 6

HWL+16. Kai He, Jian Weng, Jianan Liu, Joseph K. Liu, Wei Liu, and Robert H. Deng. Anonymous identity-based broadcast encryption with chosen-ciphertext security. In Xiaofeng Chen, XiaoFeng Wang, and Xinyi Huang, editors, *ASIACCS 16*, pages 247–255. ACM Press, May / June 2016. 4

KD04. Kaoru Kurosawa and Yvo Desmedt. A new paradigm of hybrid encryption scheme. In Matthew Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 426–442. Springer, Heidelberg, August 2004. 4, 5

KS12. Aggelos Kiayias and Katerina Samari. Lower bounds for private broadcast encryption. In *Information Hiding - 14th International Conference, IH 2012, Berkeley, CA, USA, May 15-18, 2012, Revised Selected Papers*, pages 176–190, 2012. 5, 8

Kur02. Kaoru Kurosawa. Multi-recipient public-key encryption with shortened ciphertext. In David Naccache and Pascal Paillier, editors, *PKC 2002*, volume 2274 of *LNCS*, pages 48–63. Springer, Heidelberg, February 2002. 4

KW15. Eike Kiltz and Hoeteck Wee. Quasi-adaptive NIZK for linear subspaces revisited. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 101–128. Springer, Heidelberg, April 2015. 7, 11, 15

LOS+10. Allison B. Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 62–91. Springer, Heidelberg, May 2010. 3

LPQ12. Benoît Libert, Kenneth G. Paterson, and Elizabeth A. Quaglia. Anonymous broadcast encryption: Adaptive security and efficient constructions in the standard model. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *PKC 2012*, volume 7293 of *LNCS*, pages 206–224. Springer, Heidelberg, May 2012. 3, 4, 5, 6, 7, 8, 15

Moh10. Payman Mohassel. A closer look at anonymity and robustness in encryption schemes. In Masayuki Abe, editor, *ASIACRYPT 2010*, volume 6477 of *LNCS*, pages 501–518. Springer, Heidelberg, December 2010. 4, 15

MRV16. Paz Morillo, Carla Ràfols, and Jorge Luis Villar. The kernel matrix Diffie-Hellman assumption. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part I*, volume 10031 of *LNCS*, pages 729–758. Springer, Heidelberg, December 2016. 9

NNL01. Dalit Naor, Moni Naor, and Jeffery Lotspiech. Revocation and tracing schemes for stateless receivers. In Joe Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 41–62. Springer, Heidelberg, August 2001. 3

OT10. Tatsuaki Okamoto and Katsuyuki Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 191–208. Springer, Heidelberg, August 2010. 3

Sha84. Adi Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and David Chaum, editors, *CRYPTO'84*, volume 196 of *LNCS*, pages 47–53. Springer, Heidelberg, August 1984. 4

SW05. Amit Sahai and Brent R. Waters. Fuzzy identity-based encryption. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 457–473. Springer, Heidelberg, May 2005. 3

Wee10. Hoeteck Wee. Efficient chosen-ciphertext security via extractable hash proofs. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 314–332. Springer, Heidelberg, August 2010. 4

Wee16. Hoeteck Wee. Déjà Q: Encore! Un petit IBE. In Eyal Kushilevitz and Tal Malkin, editors, *TCC 2016-A, Part II*, volume 9563 of *LNCS*, pages 237–258. Springer, Heidelberg, January 2016. 3

YFDL04. Danfeng Yao, Nelly Fazio, Yevgeniy Dodis, and Anna Lysyanskaya. ID-based encryption for complex hierarchies with applications to forward security and broadcast encryption. In Vijayalakshmi Atluri, Birgit Pfitzmann, and Patrick McDaniel, editors, *ACM CCS 04*, pages 354–363. ACM Press, October 2004. 3